UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/586,907	06/05/2000	Rajesh G. Shakkarwar	0100.0000370	9317

29153 7590 04/06/2007		EXAMINER
ADVANCED MICRO DEVICES, INC.		ZIA, SYED
C/O VEDDER PRICE KAUFMAN & KAMMHOLZ, P.C.	ART UNIT	PAPER NUMBER
222 N.LASALLE STREET		
CHICAGO, IL 60601	2131	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

	Application No.	Applicant(s)
Office Action Summary	09/586,907	SHAKKARWAR, RAJESH G.
	Examiner	Art Unit	
	Syed Zia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>27 December 2006</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) <u>1-73</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-3, 6-11, 13-26, 28-38, 40-52, 54-58, 60-64, 67 and 70</u> is/are rejected.

7)☒ Claim(s) <u>4,5,12,27,39,53,59,65,66,68,69 and 71-73</u> is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

        1.☐ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____.

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

This office action is in response to amendment filed on December 27, 2006. . Original application contained Claims 1-69. Applicant previously added new Claims 70-73. Applicant previously amended all claims 33, 64, and 67. Applicant's request for reconsideration of the finality of the rejection of the last office action is persuasive and, therefore, the finality of that action is withdrawn. Presently claims 1-73 are pending.

Response to Arguments

Applicant's arguments with respect to claim 1-73 have been considered but are moot in view of the new ground(s) of rejection.

Allowable Subject Matter

Claims 4-5, 12, 27, 39, 53, 59, 65-66, 68-69, and 71-73 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2.   Claims 1-11, 19-21, 24, 33-38, 45-47, 50, 60-61, 64, 67, and 70, are rejected under 35

U.S.C. 102(b) as being anticipated by Fisherman et al (USP 5,586,301).

As per claim 1, Fisherman et al teach a method for protection of computer assets from

unauthorized access comprising: receiving in a protection engine, an interface control command

(column 3, lines 33-36); determining whether the interface control command introduces a

security risk (column 4, lines 23-30 and column 5, lines 7-11); when the interface control

command introduces a security risk, determining a state of a switch (column 4, lines 20-33);

when the state of the switch is a protected state, inhibiting execution of the interface control

command (column 4, lines 38-42); and when the state of the switch is an unprotected state,

allowing execution of the interface control command (column 4, 20-24).

As per claim 33, Fisherman et al teach a method for protection of computer assets from

unauthorized access comprising: receiving in a protection engine in a south bridge, an interface

control command (column 3, lines 33-36); determining whether the interface control command

introduces a security risk (column 4, lines 23-30 and column 5, lines 7-11);

when the interface control command introduces a security risk, determining whether of a source

of the interface control command is authentic (column 14, 16-19); when the source of the

interface control command is not authentic, inhibiting execution of the interface control

command (column 14, lines19-24); and when the source of the interface control command is authentic, allowing execution of the interface control command (column 14, lines 25-28).

As per claims 2 and 34, Fisherman et al teach the step of inhibiting execution of the interface control command further includes the: step of: providing an indication that the execution of the interface control command was inhibited (column 6, line 65).

As per claim 3, Fisherman et al teach changing the state of the switch to the protected state when a timeout duration has elapsed (column 11, lines 50-53).

As per claim 6, Fisherman et al teach determining the state of a software-based switch (column 4, lines 29-30 and 38-42).

As per claim 7, Fisherman et al teach using cryptographic techniques to determine the state of the software-based switch (column 4, lines 25-30).

As per claims 8 and 35, Fisherman et al teach allowing data to be written to a hard disk drive (column 4, lines 23-24).

As per claims 9 and 36, Fisherman et al teach allowing data to be written to a. boot sector of the hard disk drive (column 5, lines 11-15).

As per claims 10 and 37, Fisherman et al teach allowing data to be written to a file allocation table of the hard disk drive (column 5, lines 16-22).

As per claims 11 and 38, Fisherman et al teach allowing data to be written to a floppy disk drive (column 11, lines 65-67).

As per claims 19 and 45, Fisherman et al teach determining whether the interface control command is a hard disk drive formatting command. Fisherman et al teach that the system is able to detect write operations to the hard drive (column 5, lines 7-10). Specifically the system can detect write commands to the entire cluster (column 5, lines 30-35). Also Fisherman et al teach that proposed changes are analyzed in order to prevent unsanctioned changes in the protected files and directories. Therefore, it is inherent that Fisherman et al teach determining whether the interface control command is a hard disk drive formatting command because a format function erases all data from the hard drive partition.

As per claims 20 and 46, Fisherman et al teach determining whether the interface control command is a boot sector write command (column 6, lines 64-66).

As per claims 21 and 47, Fisherman et al teach determining whether the interface control command is a program file write command (column 5, lines 26-30).

As per claims 24 and 50, Fisherman et al teach determining whether the interface control command changes a file attribute, the file attribute enabling or disabling execution of a file corresponding to the file attribute (column 13, lines 55-65).

As per claim 60, Fisherman et al teach the step of determining whether the response is valid comprises the step of: comparing the response to a mathematical function of a value accessible only to the protection engine and to an operating system (column 1, lines 63-66).

As per claim 61, Fisherman et al teach writing the value from a processor to a one-time-writable register in the protection engine (by an operating system) during a boot process (before application software is enabled) (column 1, lines 45-55).

As per claim 64, Fisherman et al teach an apparatus for protection of computer assets from unauthorized access comprising: an interface controller operatively coupled to receive a interface control command to control an interface device (column 3, lines 33-36); a switch selectable between a protected state and an unprotected state (column 4, lines 20-33);
a protection engine operatively coupled to the interface controller to receive the interface control command (see Fig. 1) and operatively coupled to the switch to detect whether the switch is in the protected state or the unprotected state (column 4, lines 29-30) to determine whether the interface control command poses a security risk (column 4, lines 23-30 and column 5, lines 7-11) and to selectively inhibit or allow execution of the interface control command by the interface controller depending on whether or not the interface control command poses the security risk and

depending on whether the switch is in the protected state or the unprotected state (column 14,

lines19-28).

As per claim 67, Fisherman et al teach an apparatus for protection of computer assets from

unauthorized access comprising: a south bridge comprising: an interface controller operatively

coupled to receive a interface control command to control an interface device (column 3, lines

33-36); and a protection engine operatively coupled to the interface controller for preventing

unauthorized access to the interface device and operatively coupled to receive the interface

control command to determine whether a source of the interface control command is authentic

and to selectively allow or inhibit execution of the interface control 5 command by the interface

controller depending on whether or not the source of the interface control command is authentic

(column 14, lines 19-34).

As per claim 70, a method for protection of computer assets from unauthorized access

comprising: receiving in a protection engine, an interface control command (column 3,line 33-

56); determining whether the interface control command introduces a security risk determined

from at least one of: a type of interface control command, an area of memory affected by the

interface control command, a device affected by the interface control command, data associated

with the interface control command, an operand associated with the interface control command,

and a relationship of the interface control command to another interface control command; when

the interface control command introduces a security risk, determining a state of a switch (Fig.1-

2, column 4, lines 23-30 and column 5, lines 7-11); when the state of the switch is a protected

state, inhibiting execution of the interface control command(column 4, lines 38-42); and when

the state of the switch is an unprotected state, allowing execution of the interface control

command (column 4, 20-24).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

3. Claims 13-17, 28-32, 40-44, 54-58 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Fisherman et al in view of Glossary of Information Technology Acronyms and Terms (here

within GITAT).

As per claims 13-16, 28-32, 40-44, and 54-58, Fisherman et al teachings controlling write access

to the hard drive (column 4, lines 20-25). Fisherman et al is silent in disclosing allowing data to

be written to a parallel port, serial port, USB port, and a IEEE-1394 port. Fisherman et al does

teach a computer system which controls data access to the system's basic input output system

(see abstract). GITAT teaches that a parallel port, serial port, USB port, and an IEEE-1394 port

are examples of computer input output ports (pgs. 138, 248, 295, and 337). One of ordinary skill

in the art would know how to control the I/O ports of a computer system. It would be

advantageous to the system's security to only allow authorized entities to have access to write

data to these ports. An unauthorized person might try to send sensitive data via an output port

whereas an authorized person may need to use the output port in a legitimate. Clearly, the

system's security would be highly stronger if the system could control access to the I/O ports.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the

invention was made to employ the teaching of GITAT within the system of Fisherman et al

because it would allow the system to grant or deny data written to I/O port, thereby greatly

improving the system's ability to monitor and control data.

As per claim 17, Fisherman et al teachings controlling write access to the hard drive (column 4,

lines 20-25). Fisherman et al is silent in disclosing allowing data to be written to a flash memory

device. GITAT teaches that a flash memory device is a nonvolatile storage chip. Hard drives are

also nonvolatile. Therefore, Fisherman et al teach controlling data written to nonvolatile

memory. Fisherman et al disclose a secure system whereby the security comes from monitoring

and controlling access to memory.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the

invention was made to employ the teaching of GITAT within the system of Fisherman et al

because it would allow the system to control data written to flash memory devices, thereby

greatly improving the system's ability to monitor and control data.

4. Claims 18, 25, 26, 51, 52 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Fisherman et al and GITAT as applied to claims 1 and 13 above, and further in view of Davis

(USP 6,205,547).

As per claims 18, 25, 26, 51, and 52, Fisherman et al teach a system controller which intercepts

commands to control the hard drive controller (see abstract).

Fisherman et al fail to teach controlling commands sent to the thermal management controller.

Davis teaches a thermal management controller which closely monitors and alters a computer's

systems thermal conditions separately from the operating system (column 6, lines 9-16). Davis

teaches that CPU fans are controlled by the thermal controller to regulate CPU temperature

(column 5, lines 40-45). Fisherman's system also works independent of the operating system so it

too cannot be influenced by processes of the operating system. Davis's thermal management

controller provides the necessary control to keep the computer system functioning properly.

Therefore, it would be highly advantageous to control which entity can write data to the thermal

controller. Clearly, commands that try to turn off CPU fans, would not be allowed be allowed by

unauthorized entities.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the

invention was made to employ the teaching of Davis within the system of Fisherman et al and

GITAT because it would permit regulation of the thermal dynamics of the system by providing a

secure method of communication with the thermal management controller.

5. Claims 22, 23, 48, 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Fisherman et al in view of Chen et al (USP 5,832,208).

As per claims 22, 23, 48, 49, Fisherman et al teaches a system which analyzes commands which

change the content of hard disks. Fisherman et al is silent in

expressing disclosing determining whether the file extension is an executable file extension

including file extensions of an exe extension, a com extension, a bat extension, or a bin

extension. Chen et al discloses a system with detects and removes computer viruses (see

abstract). Specifically, Chen et al discloses that computer viruses are attached to executable files

with an exe extension, a com extension, a bat extension, or a bin extension so that they may

infect a system (column 2, lines 8-10).

In view of this, it would have been obvious to one of ordinary skill in the art at the time the

invention was made to employ the teaching of Chen et al within the system of Fisherman et al

because it would allow the system to recognize additional types of commands that could

potentially harm the computer system.

6.   Claims 62 and 63 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Fisherman et al in view of Applied Cryptography 2"d Edition (here within AC).

As per claim 62 and 63, Fisherman et al teach the step of determining whether the response is

valid comprises the step of comparing the response to the correct response value. Fisherman et al

are silent in expressly disclosing performing a mathematical operation on the challenge to

produce a correct response value. AC teaches performing a mathematical operation on the

challenge to produce a correct response value (pg. 53). AC uses pseudorandom numbers to form the challenge value. A mathematical operation is performed on each challenge so that each authentication attempt is unique and cannot be replayed.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of AP within the system of Fisherman et al because it would allow the system to authenticate commands in which each authentication attempt is unique and highly secure.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed Zia whose telephone number is 571-272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

sz
March 18, 2007